c. a non-volatile memory mounted to said body member;

d. biometric circuitry for generating and storing in said non-volatile memory an initialized biometric template upon presentment of the person's unique biometric parameter to said biometric interface unit, and generating a second biometric template upon subsequent presentment of the person's unique biometric parameter to said biometric interface unit;

e. compare circuitry for enabling said device only if said second biometric template is substantially identical to said initialized biometric template;

f. a data storage source;

g. user interface and communication componentry for permitting said individual to store in said data storage source a plurality of indicia each one of which is representative of a secured site; and

h. password circuitry for generating a plurality of passwords, wherein each of said plurality of passwords is uniquely associated with a respective one of said plurality of indicia.

34. The device according to claim 33, further comprising indicia selection circuitry for permitting said individual to use said user interface and communications componentry to select one of said plurality of indicia when said device is enabled.

35. The device according to claim 34, further comprising recall circuitry for recalling from said data storage source the one of said passwords that corresponds with said selected one of said plurality of indicia.

36. The device according to claim 35, further comprising output circuitry and a display mounted to said body member for visually displaying said password associated with said selected indicia.

37. The device according to claim 35, further comprising an output communications port connected to said output circuitry for directly transmitting said password corresponding to said selected indicia to said secured site.

38. The device according to claim 33, wherein said password circuitry comprises a random number generator.

39. The device according to claim 33, wherein said biometric interface unit is a fingerprint reader.

40. The device according to claim 33, wherein said user interface and communications componentry comprises means for communicating a preselected string of predetermined length of characters in said data storage source.

41. The device according to claim 40, wherein said means for communicating a preselected string of predetermined length of characters in said data storage source comprises a plurality of arrow keys mounted to said portable body member which may be manipulated and actuated by said individual and which electronically communicate with said device upon actuation by said individual.

42. The device according to claim 33, further comprising means for prompting said individual to change a password corresponding to a predetermined indicia after expiration of a predetermined period of time.

43. The device according to claim 42, wherein said means for prompting said individual to change a password after expiration of a predetermined period of time comprises a clock and circuitry coupled thereto which actuates said device to display a predetermined message requiring said individual to reply in order to continue using said device.

44. The device according to claim 43, wherein said password circuitry will generate a new password and associate said new password with the corresponding one of said indicia for which said prompt was actuated.

45. A device for use by an authorized individual to obtain information for use in accessing a secured site, the device comprising:

a. a portable body member;

b. a data storage source contained in said body member;

c. user interface and communication componentry for permitting said individual to store in said data storage source a plurality of indicia each one of which is representative of a secured site; and

d. password circuitry comprising a random number generator for randomly generating a plurality of passwords, wherein each of said plurality of passwords is uniquely associated with a respective one of said plurality of indicia.

46. The device according to claim 45, further comprising indicia selection circuitry for permitting said individual to use said user interface and communications componentry to select one of said plurality of indicia when said device is enabled.

47. The device according to claim 46, further comprising recall circuitry for recalling from said data storage source the one of said passwords that corresponds with said selected one of said plurality of indicia.

48. The device according to claim 47, further comprising output circuitry and a display mounted to said body member for visually displaying said password associated with said selected indicia.

49. The device according to claim 47, further comprising an output communications port connected to said output circuitry for directly transmitting said password corresponding to said selected indicia to said secured site.

50. The device according to claim 45, further comprising means for prompting said individual to change a password corresponding to a predetermined indicia after expiration of a predetermined period of time.

51. The device according to claim 50, wherein said means for prompting said individual to change a password after expiration of a predetermined period of time comprises a clock and circuitry coupled thereto which actuates said device to display a predetermined message requiring said individual to reply in order to continue using said device.

52. The device according to claim 51, wherein said password circuitry will generate a new password and associate said new password with the corresponding one of said indicia for which said prompt was actuated.

53. A method for creating, storing, and managing a password, comprising the steps of:

a. providing a device comprising a portable body member, a data storage source contained in said body member, user interface and communication componentry for permitting said individual to store in said data storage source a plurality of indicia each one of which is representative of a secured site, and password circuitry comprising a random number generator for randomly generating a plurality of passwords, wherein each of said plurality of passwords is uniquely associated with a respective one of said plurality of indicia;

b. entering preselected indicia representative of a secured site into said device in response to a prompt generated by said device;

c. instructing said device to randomly generate a string of characters of predetermined length that is representative of a password in response to a prompt generated by said device, wherein said password is uniquely associated with said indicia entered in step b; and

d. repeating steps b and c in sequence for as many times as desired.

54. The method of claim 53, further comprising the step of instructing said device to generate a replacement password for said password created in step c in

response to a prompt displayed on said portable body member after a predetermined period of time since said password was created in step c.